FitQuest Privacy Policy

The term ‘The Gym Group Limited’ or ‘TGL’ or ‘us’ or ‘we’ refers to the operator of The Gym Group gyms, this website and the owner of this policy.

With effect from 3 February 2022 all rights to FitQuest have been acquired by TGL.

We respect the privacy of our FitQuest users.

This document outlines TGL FitQuest privacy policy (“FitQuest Policy”) with regards to the various types of user interactions and the data stored and exchanged as a result. It summarises the data we collect, the reasons why and how we process this data, together with the rights of our users under the UK General Data Protection Regulation.

If you are a The Gym Group (TGG) gym user, you are subject to the existing Membership Agreement. However, in relation to the use of a FitQuest machine or access to the FitQuest data, the terms of this TGL FitQuest privacy policy will also apply in relation to your FitQuest personal data. If and to the extent that the FitQuest Policy is inconsistent with The Gym Group’s Membership Agreement, the FitQuest Policy will prevail.

For the purposes of the UK General Data Protection Regulation (“the Regulation”) and the Data Protection Act 2018, the data owner and controller is The Gym Group Limited of 5th Floor, One Croydon, 12 - 16 Addiscombe Road, Croydon, CR0 0XT.

If you have any questions, comments and/or requests regarding this privacy policy then please contact our Data Protection Team at the following details:

- By email: dataprotection@thegymgroup.com
- In writing: 5th Floor, One Croydon, 12 - 16 Addiscombe Road, Croydon, CR0 0XT

Summary

- We need to store personally sensitive data about you, in order to provide our FitQuest service.
- We make every effort to store your data securely using appropriate and strong encryption techniques.
- We never disclose personally sensitive data to third parties (unless under a legal obligation to do so).
- We do share non-personally sensitive data (anonymised, aggregated, statistics and trends) to trusted third parties.
- We never send you spam or unsolicited email; you must opt-in to mailings of interest.

Full details on every aspect of our privacy policy can be found below.

DATA PRIVACY AND YOUR RIGHTS (GDPR)

AT TGL, WE RESPECT THE PRIVACY OF OUR USERS

We've summarised links below relating to your rights of access under the Regulation and other privacy related points of interest:

- Data Processing: In order to provide the FitQuest services and assessments, we need to process some data relating to you (some of which may be personally sensitive). Use of our services is entirely opt-in.
- Data Storage: FitQuest measurement data is stored in data centres within the EU (hosted on Microsoft Azure). Some other servers are user internationally for additional services (support, email, etc).
- Data Categories: The types of data we store are outlined in our privacy policy.
- Data Sharing: Our privacy policy outlines the circumstances under which data may be disclosed to third-parties and the recipients.
- Data Deletion: You can request we delete your account (including all measurement history) at any time. This is sometimes described as your right to be forgotten.
- Data Sources: Our privacy policy outlines the various sources from which we collect/obtain data.
- Data Profiling: We may offer insights, training tips or programmes based upon data in your profile. The results of any such profiling are accessible directly in your account. We may also use data extracts (anonymised) for research purposes (to improve our product or algorithms for example). We can exclude your data from such programmes if you prefer.
- Data Extracts: You can download history of your fitness and body composition results via our FQ score portal. Please contact us for anything further, we will endeavour to comply with reasonable requests where possible (assuming it does not adversely affect the rights and freedoms of others).
- Data Corrections: Please contact us if you feel there are errors in any data we hold relating to you.
- Complaints: Please contact us if have any complaints concerning our data collection or processing. You can also escalate your complaint to the Information Commissioner's Office (ICO), a supervisory body (https://ico.org.uk/concerns/).

- Data Protection Guarantee: For data processing within the UK & EU, we are registered with the Information Commissioner's Office (ICO) under the Data Protection Act (Registration number: Z2810154). Outside of the EU, we operate under the EU-US Privacy Shield Framework where permissible (the replacement for the EU Safe Harbor Framework).

Note: This list is not intended to be exhaustive in nature and does not affect your statutory rights.

DATA COLLECTION
We store the following types of information:

User Profile Data
This data is submitted by users into our devices, kiosk terminals, mobile/tablet applications and online website. The data listed below is explicitly requested from the user (unless otherwise stated):

- User name
- Email address
- Date of birth
- Weight - Measured automatically on kiosk terminals and some devices.
- Height
- Gender
- Organisation/Group
- Avatar
- Password
- Language and locale preferences
- Account preferences
- Related meta data

Test Measurement

Data This data is measured by our devices, applications or kiosk terminals (e.g. during a fitness assessment) or input manually by the user:

- Weight - Measured automatically on kiosk terminals and some devices
- Force platform raw data
- Body composition (BIA/BIS measurements)
- Heart rate and ECG signal
- FQ scores
- Force bar measurements
- Acceleration forces
- Related meta data

Meta Data
Non-personal data relating to usage and measurements, comprising:

- Date/time of the test measurement(s)
- The user to whom this measurement belongs
- Device/terminal identity
- Version information

Location Information
Your explicit consent is requested before gathering this type information. Location data comes in three main forms:
Locate once (to service a location based request)

Occasionally we ask your location to help service a specific request you initiated (e.g. find my nearest FQ terminal).

Your location is not stored nor associated with your account in any way. We only use the information temporarily to facilitate your request. You are always prompted for consent before your location is obtained (specifically, you are requested to enter the information manually - e.g. a town or postcode - or requested to grant temporary access to the GPS in your mobile device). This prompt or submission provides us with your location only once. Further prompts will be made each subsequent request.
Location tracking (only when manually activated by you)
You can choose to enable location tracking in some of our applications (e.g. track my run around the park).

When enabled, this type of location tracking uses your GPS to track your precise location and movements. You will be prompted for your explicit consent before such tracking is enabled, though you may disable subsequent prompts if you wish. You are free to disable tracking at any time (e.g. after finishing your run), but, as a failsafe, tracking will terminate automatically after 24 hours if you have not interacted with our application during this time. Whilst tracking is active, a visual indicator will be shown clearly in the application and in the on-going notification bar (where supported by your device). This type of location data is stored and associated with your account (so we can render a map of your run, for example).

Unintended location gathering
Occasionally we ask your location to help service a specific request you initiated (e.g. find my nearest FQ terminal).

We store information about the device/terminal used to perform each measurement to identify usage trends and detect problems or faults. We also know the geographical location of each of our terminals. We store user usage information for each terminal in case we need to contact them in relation to a problem with the terminal or in case they contact us reporting an issue. Potentially therefore, there is the ability to track an individual's location each time they sign-in to one of our terminals. Although the potential exists, we would like to make it clear we make no such attempt to track individuals in this manner. Our interest extends only to monitoring how busy each terminal is at any given time (to determine if we need more terminals at that location, for example) and identifying users who may have experienced problems with specific terminals (e.g. several users encountered problems measuring their heart rate on terminal 5).

Error Captures

All errors are captured in an effort to determine common problems and offer continuous product improvement.

The error report may contain a limited anonymised extract of test measurement data relating to the failure, to help diagnose the cause. We do not include any information that could identify you (i.e. user profile data) in our error captures. However, in rare cases, error reports may capture personal data inadvertently. Any such information is not used in any way and is discarded securely at the first opportunity.

Error reporting from our website and kiosk terminals is automatic and runs in the background without any opportunity to opt out. You may avoid signing in if this is of concern. Error reporting from our mobile applications always prompt for user consent before sending. In all cases, error reports are fully encrypted prior to transmission and stored fully encrypted.

Data captured:

- Date/time of the error
- Error category and severity
- Error description
- Events leading up to the error
- Anonymised extract of test measurement data
- Device/terminal identity
- Version information

Correspondence (e.g. Sales/Support/Feedback)

Data relating to any communication you have with us (electronic, verbal or written).

Communication sent via email, fax or general contact submission forms is not secure. Therefore, sensitive data should not be included in such mediums. We have a dedicated secure messaging facility if necessary.

We will try to categorise your communication and respond accordingly (e.g. if you request support we will offer technical help, not a sales call!). Our aim is to reply whenever possible and ensure our response is relevant.

For sales queries: we will address your questions and may send you related product/data sheets. We may follow up on sales leads to see if we can be of any further assistance.

For support queries: we will raise a support ticket and attempt to resolve your issue. This may need further communication for additional information. You may be notified of progress on a support ticket (e.g. if a fix is later made available). We may follow up after the completion of a ticket to determine if the issue was resolved to your satisfaction.

For feedback or suggestions: we may contact you to thank you for your thoughts and ideas or to request clarification on points. Your feedback may be shared with relevant stakeholders and project teams. Feedback can also be submitted anonymously if you prefer (via our dedicated feedback page). We welcome community feedback (good or bad) - it really does help shape our product offerings.

Community forums: Information submitted to our community forums is deemed to be in the public domain (unless indicated otherwise). We may use third party tools (such as UserVoice) to manage forums on our behalf.

The types of correspondence we store are as follows:

- Date/time of the communication
- User name
- Email address
- Contact telephone number(s)/fax number
- Postal address
- Response preference
- Your message
- Nature
- Language
- Timezone
- Channel information

Email

Your email address is used to identify your account and contact you.

We may send new users a welcome email to verify their new account and confirm their password and username. We will not send you unsolicited email information, commercial offers or advertisements. We will not sell, rent, or loan your email address to third parties.

Our automated emails are opt-in and sent only if you sign up to receive them (e.g. by signing up for online fitness programme or product updates). An example of an automated mail we might send after you sign up is a copy of your fitness report after performing a fitness measurement. We may also send very occasional mailings about product developments (e.g. new related products or improvements). These will be very infrequent, one or two per year at most. End-users of software products can also sign up to receive notifications about updated releases (these may be more frequent as we provide frequent update releases). We use a third-party mailing provider (such as but not limited to MailChimp or SendGrid) to send mailings on our behalf. You can opt in or out of mailings like these at any time (an unsubscribe link is included in each email sent).

We may send occasional feedback requests or surveys - particularly if the device is being used as part of a trial or beta programme. Your feedback is greatly appreciated and may be shared with stakeholders (anonymously or otherwise, as indicated in the survey). To conduct the survey independently, we may need to disclose your name and email address to a third party (such as Survey Monkey or Super Simple Survey for example). When working with third party mailing/survey companies we will link to their privacy policy here (or in the mailing) and only use third parties whose privacy policy is materially consistent with our own (i.e. ensuring they will not send you further unrelated mailings or pass your details on to other third parties). Again you may choose to opt out of such mailings if you prefer.

Unsubscribe requests are actioned immediately and no further mailings will be sent to users who have opted out.

There are some mailings which are mandatory (i.e. from which you cannot opt out). Such mailings are rare and related strictly to account servicing (i.e. are not promotional in nature). For example, we might send a security notification if we suspect your account has been compromised or authentication requests to validate sensitive requests/actions (such as a change of password). We may also notify you about important changes to our terms and conditions or policy documents. Users can only opt out of these mailings by deleting their account.

Financial Data

Data relating to financial transactions with us.

We use third party merchants (such as Nayax, Stripe, PayPal and Google Wallet) to process payments on our behalf. Please refer to the respective merchant for their privacy policies. We never store your full credit/debit card details but do keep other information related to the transaction:

- Date/time of the transaction
- User name
- Email address
- Contact telephone number(s)/fax number
- Address
- Goods/services purchased/refunded

- Transaction details

Web Identifying Data
IP Address

We log the IP address of all requests to our webservers to help maintain our security, diagnose server problems and to administer our website. For example, we use your IP to aid in the detection of malevolent actions or denial of service attacks. For certain types of request (e.g. sign-in), we also map the IP to individual accounts, particularly for failed access attempts. Such logging helps detect abnormal usage patterns and distributed brute force attacks. Occasionally, we may block access to our servers from your IP if we detect malevolent or suspicious activity. Such blocks maybe temporary or permanent.

We do not use your IP address to track any personally identifiable information.
Web Tracking and Analytics

We use website tracking and analytic tools (like Google Analytics) to determine which areas of our site users visit the most (based on traffic to those pages) and provide technology insights (like browser versions being used and device capabilities like screen resolution). We do not track what individual users read, but rather aggregated totals and statistics about user engagement (e.g. how often each page is visited, how long spent reading, etc). This helps us improve the content on our website.

Cookies
We make limited use of website cookies to help improve your website experience (e.g. to remember you on each computer if you so you chose). You can choose to remove/block these cookies in your web browser.

Some of the third party tools we use (such as Google Analytics, or financial merchants, for example) may also create their own cookies in accordance with their own respective privacy policies.
DATA SHARING, INTEGRATIONS, DISCLOSURE AND AGGREGATION
We share specific types of data with third parties in specific scenarios listed below:

Anonymised or Aggregated Data
We are working continuously to improve the algorithms and comparison scores in our product. To this end, fully anonymised extracts (i.e. without personally identifiable user profile information) are taken from test measurement data - including raw data, resulting scores and limited meta data). The anonymous data is used to compile aggregated totals, averages, statistics and trends for various gender and age groups. We may share this anonymous compiled data with third parties and stakeholders (in some cases for financial reward).

We also analyse anonymous data from each device/terminal to identify anonymised usage trends and detect problems or faults. Again this may be shared with third parties and stakeholders.

Your Results and Trends

We sometimes need to share your results and trends with third-parties, for example with your personal trainer, organisation or medic. We might share insights about your results to help deliver relevant content (e.g. training material based around your focus areas, engagement level and whether your scores are improving or declining for example. Research facilities undertaking specific research may also require access to your full results, for example data analysts. Their use of such data is governed by non-disclosure agreements. You can also choose to share your results publicly or with your friends if you wish (e.g. on social media), such actions are instigated manually by you.

Leader boards
We provide public leader boards displaying the best results (of the day or week for example). These are shown on large screens at the site or on the web - the aim being to encourage competition and engagement amongst FitQuest users. Only minimal information about you is published on the leader board (your first name, surname initial, avatar picture, city/event and your result). You can opt-out from the leader boards at any time.

Membership Systems (Sign In / SSO) We provide integrations with third party account systems to simplify the sign on process for our users. For example, we offer integrations with gym's membership systems to allow members to sign using their existing membership cards. We also integrate with online authentication platforms or Single Sign On (SSO) providers - such as Google Sign In, Microsoft Live ID, Facebook Login, OpenID, for example. This process involves the exchange of limited membership data or unique tokens - both of which identify individual users. Third party providers may track sign on and access requests. Please consult the provider's individual privacy policy for more information.

Third Party Integrations (E.g. via APIs)
We provide Software Development Kits (SDKs) and Application Programmable Interfaces (APIs) for our platform. These allow approved third party developers to integrate their systems with our own and viceversa. For example, a third party chest belt may supply information about your heart rate to us. Another example might be to combine disparate pieces of information together (combining your FitQuest results with your daily activity and diet, for example). Clearly for such integrations to happen data must be shared between the systems - including sensitive personal data. For this reason, the use of all APIs require your explicit consent. You must authorise each application wishing to integrate with your account and you are free to revoke approval at any time (preventing subsequent further access).

We also provide components (web widgets) and APIs which allow FitQuest data to be embedded in other systems. For example, your gym might display your FitQuest results in

their own membership member area - alongside your gym attendance and class bookings for example. These type of integrations are approved by TGL at an organisation wide level on your behalf (e.g for all FitQuest users at that gym).

Customer Support
To enable handling of support queries from end users and develop product improvements, approved staff have access to limited meta data about users and their tests, together with access to anonymised and aggregated data as discussed above. This limited access facilitates support and product development roles without compromising an individual's privacy.

Our staff are also able to access various account administration functions to assist users (for example to unblock an account).

However, our staff do not have routine access to an individual's sensitive personal user data, their test measurement results or security credentials (such as password or date of birth for example). Our data security systems prevent access to sensitive data unless access is explicitly granted by the individual concerned.

Legal Obligations

We will disclose all of your data (securely) to third parties when under a legal obligation to do so. For example, to law enforcement agencies upon receipt of a valid court order.

STORAGE AND SECURITY
We use the latest server, database, backup and firewall technologies to protect the data we store. Our data is housed in secure data centres, with both physical access restrictions and network security restrictions in place. Access to backup media is also controlled and redundant media is wiped securely or physically destroyed. We endeavour to keep abreast of OS and application updates, security fixes and keep our knowledge current about new types of exploit.

We encrypt sensitive data on the machine (such as user names, email addresses and date of birth) and transmit it to our servers securely. We store user passwords using strong one-way cipher hashes (uniquely salted) recommended for passwords. We guard against known attack vectors (such as SQL injection, crosssite scripting attacks, etc) and employ 'defence in depth' strategies (i.e. multi-layers of defence) following industry best practice security guidelines (like OWASP) wherever possible.

Our general staff have no access to sensitive user profile data or an individual's test measurement data (although some meta data, aggregated data and anonymised results are made available to authorised personnel - see also the dedicated data disclosure section above). We also take steps to ensure computers outside of the data centres are kept secure (to guard against employee accounts being compromised for example).

We develop to dedicated developer and staging servers. To prevent errors during development exposing user data, our developer servers do not contain live user data, only dummy data. Our FitQuest source code is version controlled so we can track change history and audit who worked on individual pieces of code.

We use some data centres outside of the UK/EU area, specifically in the US. We continue to be the owner of this data and ensure these operators have robust data privacy policies, materially compliant with our own and/or compliance with the EU-US Privacy Shield Framework (formerly the EU Safe Harbor Framework).

If you find a security weakness in our site, we urge you to contact us privately before disclosing it publicly - to give us the opportunity to fix it. We are happy to give you public credit for such disclosures made responsibly in this manner, once a fix has been made available.

Should we discover a data breach of our system (or be made aware of one), we pledge to notify the ICO supervisory body and affected users in a timely manner without undue delay.

CHILDREN

We have a social conscience and one of our goals is to improve the fitness of the whole nation. We believe engaging the next generation is crucial. Accordingly, children are welcome to use FitQuest, but we ask they do so under supervision and with parental consent. Note our algorithms do not currently provide normative values for children and access to certain features may be restricted for minors (such as chat forums for example).

We are looking for ways to work with schools to measure entire year groups to gain greater insight into children's fitness levels and normative ranges. Any of our employees working with children are vetted for a criminal record (DBS) and all measurements in school are undertaken jointly with the school, under teacher supervision.

ACCOUNT DELETION

You are free to delete your account at any time (‘your right to be forgotten’) - just contact us.